Council Working Group on International Internet-related Public Policy Issues
Sixteenth meeting – Virtual meeting, 23 September 2021

Document CWG-Internet-16/4-E
9 September 2021
English only

Contribution by the Russian Federation

RISK ANALYSIS OF THE EXISTING INTERNET GOVERNANCE AND OPERATIONAL MODEL

1. Introduction

At the 15th meeting of the CWG-Internet, held in January 2021, the Russian Federation proposed to discuss aspects related to Internet governance with focus on critical infrastructure, including resources supporting the system of domain names and internet addresses. Continuing this issue, we would like to present our vision of the threats and risks of the existing Internet governance and operational model.

2. Discussion

First of all, it should be noted that today the development of telecommunications/ICT services based on the Internet is of great importance both for humanity as a whole and for an individual state. Thanks to Internet significant progress has been made in the development of scientific knowledge, education, medicine, economics and other areas. At the same time, the proper functioning of the national domain of the Internet and its reliable connection and integration with the global network has become a vital function for any state, economy and population.

And here the question rightly arises: is the existing Internet governance system able to cope with potential threats to the integrity and resilience of the network, to give a worthy response to such a global challenge? Internet emerged as a research project and at the initial stage existed in the academic environment on the self-organization basis. The institutionalization of Internet governance mechanisms was carried in the mid-1990s and was adequate to the scale and importance of the Internet at that time. Since then, the importance, scale and level of penetration of Internet services in all areas of life: public services, economy, daily life of people, have increased many times, but the principles and mechanisms of governance the global network have remained the same.

The Russian Federation has repeatedly expressed concern on the lack of reliable guarantees for the Internet development and security at various international platforms. Currently, there is not a single international legal act that would guarantee the integrity and

security of the Internet's public core, and without such fundamental instruments, it is impossible to ensure the long-term and productive development of the Internet and its services globally.

The key threats to the security and stability of the existing governance and operational model of the Internet are the lack of international status of organization-operators of critical infrastructure and lack of international legal acts guaranteeing immunity of its operational activity, as well as the lack of effective international regulation of digital services. Prepared by a working group of Russian experts: representatives of the Internet industry, government bodies, technical and scientific experts "Risk Analysis of the Existing Internet Governance Model" is given in Appendix No. 1

These threats can cause numerous critical risks for national segments of the Internet and for the integrity, resilience and security of the global network as a whole. Now, certain aspects of regulation are divided between various organizations and their efforts are largely uncoordinated, while the complexity of regulation requires close international cooperation of all stakeholders. The COVID-19 pandemic naturally led to increasing the role of state as a mechanism of public organization, as well as the role it plays in the life of society. At the same time, the scale of challenges for global network connectivity is such that neither Internet giants (Big Tech), nor entire sectors of the Internet economy can deal with them properly. In the context of an aggravated international situation, Internet space uncontrolled militarization and cybercriminals significantly increasing their strength for attacking the global infrastructure, it is the states that must act as guarantors of the stability and integrity of the Internet's public core.

3. Proposal

The tasks of the CWG-Internet are Identify, study and develop matters related to international Internet-related public policy issues. ITU Council Resolution 1305 defining the public policy issues to be addressed in the CWG-Internet contains the topic “The security, safety, continuity, sustainability, and robustness of the Internet”. Thus, within the ITU's mandate, this makes appropriate to organize work on the analysis of risks of the existing governance and operational model, preparation of recommendations and further draft international legal acts in line with ITU responsibility.

Within the framework of the theme “The security, safety, continuity, sustainability, and robustness of the Internet” it is proposed:

1. Conduct the following open consultations with all stakeholders on the topic "The role of states in ensuring the integrity, resilience and stability of the public core of the Internet and the need for international legal acts to guarantee the integrity, resilience and stability of the public core of the Internet".

2. Invite Member States to submit at the 17th CWG-Internet meeting their vision of the risks of the current Internet governance and operational model.

3. Invite Member States to submit at the 17th meeting of the CWG-Internet their views on possible ways to overcome existing challenges and mitigate risks in the governance of critical infrastructure of the Internet for future discussion.

4. Invite Member States to present at the 17th meeting of the CWG-Internet their views on the preparation of international legal acts to overcome the existing challenges and risks in the management system of Internet critical infrastructure to guarantee the integrity, stability and security of the Internet public core.

5. Organize within the Working Group discussion and preparation of recommendations for ITU Consul based on the materials submitted by the Member States and all stakeholders on the above issues.

For the definition of the “public core of the Internet”, see in the Appendix No. 2 “DEFINITION OF THE PUBLIC CORE” prepared by the Global Commission on the Stability of Cyberspace (GCSC).

Appendix 1

Risk analysis of the existing Internet governance and operational model

Risks to Infrastructure under the Current Internet governance and operational model

№	Name of risk	Explanation	Expressed by
For international Internet segment			
1.	**Restrictions on access to internationally used infrastructure (violation of non-discriminatory access)**	Any user/Internet provider/operator should be provided with access to internationally used infrastructure on an non-discriminatory basis, however, currently transit or IXP operators do not have any guarantees of noninterference with their operational activities. “Global connectivity” should be neutral and have immunity, legal access restriction on national level.	Disconnectivity and disintegrity of the global network
			The user does not receive a service from a certain service providers or operators.
2.	**Transit traffic manipulations**	No guarantees for the stable operation of the main nodes of the Internet (Internet exchange points, top-level domain servers, root servers and etc.), and obligations to no n-interfere with transit traffic transfer and to preserve confidentiality of communications during packet-based data transfer.	Unauthorized analysis and interception, monitoring and prioritization of certain types of traffic by both operators and national law enforcement authorities
			Violation of net neutrality principle – some communication channels enjoy higher priority than the others

3.	**Dependence on decisions of a national administration**	Critical infrastructure operators/ organizations (ICANN, PTI, RIRs, etc.) may be forced to comply with sanctions of a national administration under which jurisdiction they are located. A number of operational organizations performing supranational functions in the Internet governance are registered in the USA, and they must comply with all laws, rules and regulations of the US judicial authorities as well as of the Office of Foreign Assets Control (OFAC).	Decision of a national administration may restrict or affect the accessibility of the Internet services in other countires.
4.	**Lack of effective mechanism for the joint work of national Administrations and Regional Internet Registries (RIR)**	Lack of active legal mechanisms to resolve resource allocation disputes	Unequal allocation of numbering resources among States in the same region (pools of IP-addresses).
			Revocation of the Local Internet Registry status (the right of a certain service provider to allocate IP addresses and provide registration services).
5.	**Prevailing of business community's interests over the public interests**	Prevailing of business community's interests over the public interests, for example, when considering disputes concerning geographical domain zones/domain names, the impact of interested States and States in general is limited (precedents related to ".amazon", country code on second level domains).	Transfer of domain names to corporate entities to the detriment of the interests of the state/public (the preservation of national and cultural heritage, identity of the territory and language)
6.	**Lack of equal distribution of critical infrastructure worldwide**	Geopolitical and technical risks	In case of technical/network failures within one country there is a probability to lose a linkage with the key elements.

			Global natural disasters (earthquakes, floods, and fires) may also affect. Sanctions policy implemented by countries of location of the critical infrastructure.
7.	**Revocation of Digital security certificates that authenticate the web site you are navigating**	Restrictions of a national administration for SSL-Certificates Provider(s) create a risk of revocation of certificates for the other national zones in which they are used. However, local certificates are not recognized by global software and service providers.	Root certification centres have no mechanisms for monitoring and accountability, and in their activities are governed by domestic standards; revocation of Root Digital Certificates is possible that would fail the authorization system in the national segment and, as a consequence, the operation of Internet services, and access to web sites.
For national Internet segment			
1.	**Using DNS encryption protocols (DoH, DoT) enabling concealment of name (identifier) of an Internet resource**	Technical difficulties in provisioning public interests related to protection of the national Internet segment from illegal activities	Reducing the efficiency of using the current systems for filtering illegal content
			Difficulty to block websites with illegal content by communication service providers
			Impossibility to configure parental control in browsers
			Impossibility to analyze network behaviour infected with malicious software and to combat it
			Difficulty in managing the Lawful Interception (LI) within the national Internet segment
			Leakage of financial information or trade secrets, theft of funds

2.	**Using certain encrypted DNS servers (DNS resolvers) in browser settings that cache IP addresses**	Degradation of quality inherent in the global DNS – decentralization. Redirecting DNS traffic to a single encrypted DNS resolver specified in the browser settings.	Decreasing the role of root servers under the auspices of ICANN
			A threat of "privatization" of the key Internet infrastructure by major players
			Concentration of Big Data collected about users by encrypted DNS resolver operators
3.	**Restrictions on domain name registration** **Restrictions on obtaining IP addresses**	Entities allocating IP addresses may be forced to comply with the sanctions imposed by a national administration under which jurisdiction they are located	Lack of Internet identifiers (IP addresses) at national registrars' and service providers' which are available for allocation to users, slowdown in the development of national Internet segment
4.	**Distortion of records in databases of regional Internet registries, data corruption in the DNS root zone, and data corruption in the List of Root Certificate Authorities, and so on**	Operators of critical elements of the Internet basic core may be forced to comply with the sanctions imposed by a national administration under which jurisdiction they are located	The State is not independent in managing its online resources (IP addresses, domain names)
			Depriving a country of unique Internet identifiers creates a potential threat to the stability and integrity of the national segment of the Internet.

Content Risks under the Current Internet governance and operational model

№	Name of risk	Explanation	Expressed by
For international Internet segment			
1.	**Manipulation of application service traffic**	Manipulation of application service traffic	Violation of net neutrality principle – some communication channels enjoy higher priority than the others
			Unauthorized analysis and interception, monitoring and prioritization of certain types of traffic
2.	**Lack of an international platform to solve practical issues and discuss service challenges**	ICANN deals with the domain name system IP addressing only,while RIPE NCC deals with IP addressing only. But there are also other issues, i.e. personal data protection, encryption, identifying and blocking illegal content, universal authentication, etc. These aspects extend to different organizations or uncovered on international level.	Growth of cybercrime
3.	**Digital Monopoly,** **privatization of the Internet**	Market dominance of the largest service providers to the detriment of healthy competition and public interests.	The largest IT giants dominate the market by driving out or buying up the alternative service providers, leaving no free choice in type and terms of services to the end user, i.e. zero-option choice.
4.			Restrictions in the provision of services

5.	**Dependence on decisions of national administrations**	Dependence of global providers on decisions of national administrations in the countries of registration of their head offices.	Limited influence of states in the processes of policy-making and coordination for digital monopolies.
6.	**Prevalence of corporate standards and rules over public interests and their non-transparency**	Operation of search engines, censorship and illegal content combating are regulated by the company's own criteria.	The largest IT giants do not just sell goods and services, but shape customer preferences, make choice for them, often deprive people of the right to choose, offering them convenient, efficient, but zero-option services. The largest IT giants block content based on their own criteria rather than legislation of the countries, in which national segments of the Internet content is distributed.
For national Internet segment			
1.	**Using encryption in applications**	The use of encryption in applications	Reducing the efficiency of using the current traffic filtering systems
			Difficulty in the work of international law enforcement organizations in combating general crime. Technical difficulty in managing Lawful Interception (LI) activities.
			Difficulty to block services with illegal content by communication service providers

2.	**Lack of universal authentication/identification systems**	Impossibility to identify the source of illegal actions. Impossibility to create globally the services that require “critical information” – medical data, financial services, etc.	Potential risk of fraud, when attackers gain access to confidential information disguised as its owners.

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

www.cyberstability.org | info@cyberstability.org | cyber@hcss.nl | @theGCSC

DEFINITION OF THE PUBLIC CORE, TO WHICH THE NORM APPLIES

Bratislava, May 2018

In November, 2017, the Global Commission on the Stability of Cyberspace (GCSC) issued its *Call to Protect the Public Core of the Internet*:

> **NON-INTERFERENCE WITH THE PUBLIC CORE**
>
> **Without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.**

As input to its process, a working group of the GCSC conducted a broad survey of experts on communications infrastructure and cyber defense to assess which infrastructures were deemed most worthy of protection. On a scale of zero to ten, with zero being "unworthy of special protection" and ten being "essential to include in the protected class," all surveyed categories ranked between 6.02 and 9.01. Accordingly, the Commission defines the phrase "the public core of the Internet" to include packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, and physical transmission media. Specifically:

Packet routing and forwarding include, but are not limited to: the equipment, facilities, information, protocols, and systems which facilitate the transmission of packetized communications from their sources to their destinations. This includes Internet Exchange Points (the physical sites where Internet bandwidth is produced) and the peering and core routers of major networks which transport that bandwidth to users. It includes systems needed to assure routing authenticity and defend the network from abusive behavior. It includes the design, production, and supply-chain of equipment used for the above purposes. It also includes the integrity of the routing protocols themselves and their development, standardization, and maintenance processes.

Naming and numbering systems include, but are not limited to: systems and information used in the operation of the Internet's Domain Name System, including registries, name servers, zone content, infrastructure and processes such as DNSSEC used to cryptographically sign records, and the whois information services for the root zone, inverse-address hierarchy, country-code, geographic, and internationalized top level domains and for new generic and non-military generic top-level domains.

It includes frequently used public recursive DNS resolvers. It includes the systems of the Internet Assigned Numbers Authority and the Regional Internet Registries which make available and maintain the unique allocation of Internet Protocol addresses, Autonomous System Numbers, and Internet Protocol Identifiers. It also includes the naming and numbering protocols themselves and the integrity of the standardization processes and outcomes for protocol development and maintenance.

The cryptographic mechanisms of security and identity include, but are not limited to: the cryptographic keys which are used to authenticate users and devices and secure Internet transactions, and the equipment, facilities, information, protocols, and systems which enable the production, communication, use, and deprecation of those keys. This includes PGP keyservers, Certificate Authorities and their Public Key Infrastructure, DANE and its supporting protocols and infrastructure, certificate revocation mechanisms and transparency logs, password managers, and roaming access authenticators. It also includes the integrity of the standardization processes and outcomes for cryptographic algorithm and protocol development and maintenance and the design, production, and supply-chain of equipment used to implement cryptographic processes.

Physical transmission media include, but are not limited to: physical cable systems and installations for wired communications serving the public, whether fiber or copper. This includes terrestrial and undersea cables and the landing stations, datacenters, and other physical facilities which support them. It includes the support systems for transmission, signal regeneration, branching, multiplexing, and signal-to-noise discrimination. It is understood to include cable systems that serve regions or populations, but not those that serve the customers of individual companies.

Some experts believe that far more categories of Internet and ICT-enabled infrastructure are deserving of protection, so this definition may be broadened in the future.